

SECURE VIRGINIA INITIATIVE PROGRESS REPORT

The Honorable John H. Hager
Assistant to the Governor for Commonwealth Preparedness

July 30, 2002

On January 31, 2002, Governor Mark R. Warner signed Executive Order 7 establishing the Secure Virginia Initiative. The responsibilities charged to the Initiative are generally summarized as follows:

“Improve the Commonwealth’s preparedness and response and recovery capability for natural disasters and emergencies of all kinds, including terrorist attacks.”

Concurrent with the charge were eight primary activities outlined in the Executive Order. This progress report includes a discussion of each activity focusing on general work effort and a status update.

Secure Virginia Panel

This Panel serves as the broad policy analysis tool for the Commonwealth’s overall efforts. The Panel has been divided into nine sub-Panels and is supported by the members of the Commonwealth Preparedness Working Group (CPWG), a standing multi-agency cross Secretariat group of senior state agency officials.

“The Panel shall review, evaluate and make recommendations relating to emergency preparedness of government at all levels within the Commonwealth. Additionally, the Panel shall facilitate cabinet level coordination among the various agencies of state government related to emergency preparedness and will facilitate private sector preparedness and communications.”

The Panel has conducted four official meetings to date. The initial two meetings were designed to establish the foundation for the Panel’s overall effort, provide a consistent level of understanding concerning threats facing the Commonwealth as well as the structure for responding to and recovering from emergencies and disasters. Two meetings of the full Panel were dedicated to functional areas being considered by the various sub-Panels: transportation and cyber/technology and critical infrastructure issues. Future meetings will be oriented towards the remaining areas of emphasis of the sub-Panel’s and on a dynamic set of recommendations from each sub-Panel to present to the Governor.

Statewide Forum

Executive Order 7 directed that a summit of the key stakeholder groups be convened to discuss the Commonwealth’s level of readiness and to solicit input on areas requiring improvement.

On April 3, 2002, the Secure Virginia Initiative Forum was held in Richmond. In attendance were over 250 professionals representing the key stakeholder groups:

- Emergency Management
- Fire
- Emergency Medical Services
- Law Enforcement
- Financial Services
- Health Care
- Technology
- Transportation
- Utility
- Agriculture

The attendees provided valuable input that has been shared with the full Panel and will be considered in its deliberations through the First Responders and other sub-Panels. In addition, the summary of input was developed following the meeting and shared with all attendees as a means of establishing continuing dialogue on issues affecting Commonwealth Preparedness.

Agency Continuity of Operations (COOP) Plans

All Executive Branch agencies were required to submit to our office by May 31, 2002 their operational plans that guide emergency response activities to include Continuity of Business Operations.

All agencies, including colleges and universities have complied. Staff are in process of reviewing these plans and will be providing feedback to each agency.

Citizen Preparedness and Involvement

This office was charged with enhancing citizen involvement in preparedness and ensuring effective outreach to local governments.

Efforts are progressing to outline a viable approach to implementing the USA Freedom Corps initiative in Virginia. Our goal is to ensure effective coordination between the various components of Freedom Corps: Americorps, Senior Corps, Citizen Corps and Peace Corps. This office has been designated as the lead for Citizen Corps and its four major components: Volunteers in Police Service (VIPS), expanded Neighborhood Watch, Reserve Medical Corps and Community Emergency Response Team (CERT) training. Our office is working with responsible state agencies and Cabinet officials on each component of Citizen Corps. A proposed overall approach to USA Freedom Corps in Virginia is under development.

Effective outreach has been a focal point of our Secure Virginia efforts. In addition to the April Forum our office has participated in more than 200 meetings and appearances with constituent groups, to include vendors, since Secure Virginia was initiated. This

outreach has been invaluable in assisting our efforts to structure statewide government activities. Two key goals in this effort are informing constituents to reduce fear and raise awareness and promoting economic enhancements by positioning Virginia communities and businesses to capitalize on federal funding opportunities.

Grants Coordination

Executive Order 7 included a tasking to ensure coordination of federal grants related to preparedness.

This effort has moved forward with a good level of cooperation among state agencies. It should be noted that the federal '02 budget contained only initial funding for preparedness related activities. To date our office has ensured coordination of grants to address Health and Medical, Port Security, First Responder, Citizen Corps and Agricultural issues. It is expected that the federal '03 budget will result in at least 60-70 million dollars in first responder grants being made available to the Commonwealth. We are working closely with responsible state agencies to ensure processes are in-place to rapidly apply these funds to meet identified statewide needs, especially at the community level.

Local – State – Federal – Private Coordination

Improving the Commonwealth's preparedness requires unprecedented cooperation between local, state, federal and private sector organizations, a charge included in Executive Order 7.

In light of the Commonwealth's ongoing preparedness efforts prior to and subsequent to September 11, operational coordination among the three levels of government has been effective. Since the inception of the Secure Virginia Initiative efforts have focused on enhancing policy level relationships with Congress, the White House Office of Homeland Security and other stakeholders. This effort has been successful as evidenced by Virginia's overall competitiveness for funding, improvements in coordination of National Capitol Region preparedness and interaction with OHS, NGA and other organizations.

Additional focus will be placed on coordination of private sector activities. There are two key elements. We must enhance Virginia's ability to leverage expertise resident in the state (especially Northern Virginia) to address some of our more complex preparedness challenges. Also, it will be critical that we improve our planning and information exchange with private sector players to provide more operational level coordination. Improvements will require adjustments in both policy and statute. These issues are being considered by the Secure Virginia Panel.

Operational Plan

This office is also required to evaluate the effectiveness of the Commonwealth's plans that guide our response to and recovery from emergencies and disasters, including terrorism.

This effort is on-going. The Commonwealth of Virginia Emergency Operations Plan (COVEOP) is maintained by the Department of Emergency Management but reflects the

operational goals of all state agencies with attendant responsibilities. A review of this plan, both in terms of its strategic application and the individual responsibilities of state agencies, is progressing. The full Secure Virginia has been briefed and recommendations for modifications or changes will be completed by January 31st, consistent with the Executive Order.

Strategic Plan

The ultimate efforts of the Secure Virginia initiative are focused to support the development of a statewide strategic plan and implementation approach to guide preparedness activities.

This is clearly the most challenging aspect of the Secure Virginia initiative. There are substantial issues that are being considered by federal agencies and these will have direct impact on how Virginia approaches its overall preparedness during the next three years. Efforts are proceeding to design and develop a strategic plan building on statewide target and threat assessments already conducted, previously identified equipment, training and exercise needs and Virginia's local and state level structure for addressing emergencies and disasters, including terrorism. The long promised National Strategy has been released and Congress should complete its work on the federal '03 budget by early fall. Consequently, there should be sufficient visibility of federal efforts that can be combined with state activities to finalize an overall strategic plan for the Commonwealth prior to the end of the year.

The current proposal for the Virginia strategy will include a comprehensive "all-hazards" approach with emphasis on terrorism and homeland security issues. The proposed major elements of the strategy will include:

- Crisis (Law Enforcement) and Consequence Management Challenges facing Virginia
- Internal and External Threats and Capabilities
- Preparedness Capabilities and Needs
 - Planning
 - Training
 - Exercising
- Response Capabilities and Needs
- Recovery Capabilities and Needs
- Mitigation, Prevention and Deterrence Capabilities and Needs

These categories will be consolidated into a single long-term strategy to guide preparedness activities in Virginia.

Guidance Issues:

The Panel identified early the need to provide Governor Warner with continuing informed recommendations throughout the process rather than to simply wait until its overall effort had been completed. This decision was guided by several factors including the potential need for the development of legislation or budget requests during the upcoming session of the Virginia General Assembly as well as the need to immediately develop and sustain momentum on preparedness issues.

RECOMMENDATIONS SECURE VIRGINIA INITIATIVE UPDATE

1. Background Checks for Public Sector Employees in Sensitive Positions

Most local government and state agency organizations do not require criminal background checks for employees with exception of those in law enforcement related positions. Consequently, individuals hired to perform activities at critical government facilities such as transportation centers, water filtration plants or electric distribution stations may be hired with only the normal hiring screening process. It is recognized that the sensitivity of these types of positions necessitates a more rigid screening process. Agencies do not presently uniformly require criminal checks for personnel. This presents a possible vulnerability, in that personnel who are untrustworthy may be unknowingly hired and placed in positions that allow access to sensitive information or critical functions.

BACKGROUND:

Performing National Crime Information Center (NCIC) checks through the FBI for other than criminal justice purposes requires explicit authority to be granted. As most agencies do not have this authority, individuals hired to perform activities at critical government facilities such as transportation centers, water filtration plants or electric distribution stations may be hired with only the normal hiring screening process. It is recognized that the sensitivity of these types of positions necessitates a more rigid screening process in many cases.

ACTION:

Governor Warner has approved a proposal to allow for criminal background checks for sensitive positions in State and local government. The proposal will be developed in accordance with applicable federal guidelines to allow for part of the screening to include National Crime Information Center checks.

2. *Employer Validation of Foreign Workers Eligibility*

BACKGROUND:

- ❑ What is known as the I-9 Process was established in 1986-1987.
- ❑ Handbooks and forms were mailed to all employers in 1986 and 1987.
- ❑ The I-9 form has sections to be completed by the employee and employer. The employer checks employee identification and other records.
- ❑ The Virginia Employment Commission has or can get the forms.
- ❑ The I-9 form is titled U.S. Department of Justice, Immigration and Naturalization Service (INS), Employment Eligibility Verification. It is numbered OMB 1115-0136, and was revised 11-21-91.
- ❑ The Handbook for Employers, Instructions for Completing Employment Eligibility, is dated 11-21-91. The Department of Justice, Immigration and Naturalization Service stopped publishing the book. A new publication is anticipated.
- ❑ Documents presented to the employer must pass two tests.
 - ✓ Appears genuine.
 - ✓ Relates to the individual presenting the documents (appears to be issued to the person presenting the documents).
- ❑ Employers must not use the process to discriminate. Apply the same criteria in the same manner to each potential employee.
- ❑ If the documents do not appear genuine or do not appear to relate to the individual presenting them, the employer may state that he does not doubt the potential employee, but has concerns that must be satisfied to meet his obligations. The employer expresses those concerns and recommends that the potential employee get INS to make corrections. If the individual is in the U.S. legally and wants the job, they will comply.
- ❑ Social Security Service has sent employers a list of name and number mismatches. This does not necessarily indicate misrepresentation on the part of the potential employee. If the employer is aware of a name/number mismatch, he should request that the potential employee get the mismatch corrected.
- ❑ The Office of Business Liaison, INS Headquarters in Washington, D.C. will help an employer with the “appears genuine” test. If an employer has doubts and wants help, documents may be faxed to (202) 305-2523 for review by an INS employee. Both sides of the form need to be sent.

ACTION:

Governor Warner has directed that relevant training be provided.

3. *Emergency Alert System Enhancements*

BACKGROUND:

The Emergency Alert System (EAS) is the current version of the former Emergency Broadcast System (EBS), which was developed and designed during the Cold War era to allow the President of the United States to communicate directly with Americans in a National Emergency (i.e. a strategic nuclear attack against the continental U.S.). Thankfully, to date, there has been no need for the President to utilize the system for this purpose. There are other permissible uses of the system at the national, state, and local levels for natural disasters and other emergencies. The activation of the system for non-Presidential emergencies is however, strictly voluntary on the part of broadcasters. The Federal Communications Commission (FCC) regulates the operation of EAS. There is a “State Emergency Communications Committee” (SECC) in each state, which is responsible to the FCC for developing an EAS Plan specific to that state and for overall coordination of the EAS within that state. The SECC Chairperson is an FCC-appointed position.

The design of the current EAS reflects its origin during the Cold War era; the best technology of the times required a system of relays by high-powered AM broadcast radio stations of a signal originating at the White House and fanning out to stations in each state. These “state primary” stations would then re-broadcast the alert message, which would be picked up by other stations (“state relay” stations) monitoring the primary station, which would then re-broadcast that message to other stations (“local primary” stations) monitoring them. In this “bucket brigade” fashion, a message could be sent from the national level to localities and heard by citizens monitoring radio (and eventually television and cable systems). This is still the primary method of operation across the U.S.

The EAS works fairly well at the local level. Typically, the EAS is activated on a routine basis by the National Weather Service (NWS) for severe weather events. Participating EAS stations constantly monitor the NWS NOAA Weather Radio for weather alerts and re-broadcast those EAS alerts affecting their listeners/viewers routinely. Modern technology used in the current EAS allows for those jurisdictions affected by an event to be encoded into the EAS message in order to activate only those receivers in the threatened area. Note: the signal of the radio, television, or cable system carries the EAS alert to all areas within its range, but alerting receivers will only “activate” for the areas programmed if they are encoded into the message itself.

Beyond the local area however, the EAS system is not reliable. This is due to many reasons including changes in station ownership and sense of priority about the EAS, changes in location of stations and method of operation, lack of enforcement on the part of the FCC, and the simple fact that participation is voluntary. However, even if participation was 100%, the “bucket brigade” nature of the current system causes a statewide EAS message to take several hours to transit the entire Commonwealth. If one or more key relay stations fail to monitor and receive a EAS message or decide

not to re-broadcast it, the entire relay system potentially fails. There is a requirement to quickly activate and alert the state-level EAS for multi-jurisdictional, regional, and statewide emergencies (large hazmat incidents, terrorism, etc.). The current EAS does not fulfill the requirement.

A method to rapidly activate and disseminate a state-level or statewide EAS message to the state primary station, state relay stations, each local operational area primary station, and each of five National Weather Service offices serving Virginia is required to ensure that Presidential and Gubernatorial EAS messages can be effectively transmitted. The system must be compatible with equipment currently in use across the U.S. for EAS encoding/decoding/reception and re-broadcast and must provide for eventual changes in event codes and other technical parameters. The system must provide a reasonable level of system and message security to prevent potential “hacking” and transmission of false EAS messages.

ACTION:

Governor Warner has approved the first phase of a plan to provide satellite-based emergency messaging system that provides the capability to transmit an EAS message to an individual station or a group of stations, simultaneously and instantaneously. The system must provide for secure transmission and acknowledgement to ensure reliability. Such a system is currently available and is being considered for use by the states of Maryland, North Carolina and the District of Columbia. Federal funding will support this effort.

4. **Designation of Permanent Web-site for Communicating With the Public During Emergencies and Disasters**

BRIEF DESCRIPTION OF ISSUE OR PROBLEM:

Virginia needs a single information source where citizens and media can go to learn about terrorism preparedness and what to do in the event of an attack. The primary advertised information source should be a state-maintained Web site, which can carry continuously updated content for Virginians to access. Currently the Virginia Department of Emergency Management Web site at www.vaemergency.com serves as that information source. However, to fully meet the requirements of communicating to high volumes of people during a major crisis, funding is necessary to enhance the existing site and to provide adequate staffing for 24/7 high usage crisis periods.

BACKGROUND:

Past disasters to include the 9/11 terrorist attack have clearly illustrated that citizens seek information via the Internet/Web. Since 1996, the Virginia Department of Emergency Management has had a strong presence on the Web. Their site, www.vaemergency.com, has been recognized nationally for its content, ease of use, interactivity and up-to-date information. The site is fairly well known among citizens, the media and local governments. Currently, a P-14 wage employee at VDEM manages the Web site. A portion of the site development is done by an outside contractor. During emergencies such as the 9/11 Pentagon attack and Hurricane Floyd, the Web site experienced a 320 percent jump in usage.

The VDEM Web site has performed a significant service to citizens and the media during past emergencies and disasters. However, during a major terrorist event or catastrophic natural disaster, the current staffing, infrastructure, content, hardware and software would not be sufficient to meet the high demand for information.

ACTION:

Governor Warner has approved use of federal funding an upgrade of the vaemergency.com web site so that is complete, more fully interactive and will become the first point of reference for anyone seeking the latest information about terrorist activity or any other Virginia emergency. The annual cost of such an upgrade to include hardware, software, Web development, maintenance and staffing is estimated at \$100,000.

5. Technology Improvements

BRIEF DESCRIPTION OF ISSUE OR PROBLEM:

Commonwealth computer incidents, including web site attacks, attempted unauthorized access to databases, and malicious corruption of code, have increased in number over the past years. While some of our larger organizations have excellent defenses against these intruders, others are wanting in this highly skilled area. Some communities and business partners are also in this category. Failure to prevent or to contain intrusions can potentially result in the inability to access needed information in a timely manner and thereby our ability to respond to emergencies. In addition cyber attacks can result in financial loss, noncompliance to State and Federal statutes (e.g., HIPAA), degraded customer service, or loss of public confidence.

BACKGROUND:

Over the past two years, the following five significant events have positioned the Commonwealth to take the next steps necessary to prepare for and protect against cyber attacks:

- 1) May 2001 - The Commonwealth's first Security Architecture document was published by the Secretary of Technology. This foundational document provides a framework for consistency, coordination, and collaboration in applying security safeguards across the entities in the Commonwealth, while providing the latitude to use risk-based decision-making processes to determine the appropriate level of protection and product types.
- 2) May 2001 - A \$9 million dollar Commonwealth Information Security Center was established by the Governor at James Madison University, in partnership with George Mason University, Virginia Polytechnic Institute and Hampton University. The objective of the center is to become a leading provider of information security services and research.
- 3) December 2001 - The Secretary of Technology published an Information Technology Security Standard and Guideline for state agencies, higher education and local government.
- 4) January 2002 - Executive Order 7 required that all agencies develop/update and file a Business Continuity Plan with the Governor's office no later than May 31, 2002.
- 5) March 2002 - House Bill 823 empowered the Secretary of Technology to conduct technology security audits, which will be used to assess progress in moving towards said architecture and standard.

ACTION:

The Governor has approved initiation of a program that supports movement towards the Commonwealth's Security Architecture and Standard. The Department of Technology Planning has proposed a best practice model that calls for the establishment of a statewide security structure which provides the following core services:

- Critical IT Infrastructure Assurance
- Incident Alerts and Reporting
- Incident Response Assistance
- Incident Resolution
- Penetration Testing
- On-site consulting
- Procurement contracts
- Product and Services Review
- Best Practices Review
- Security Program Audits
- Proactive Training and Certification
- Security Awareness Promotion

Governor Warner has directed that the Secretary of Technology work with the Center for Secure Information Systems (GMU) and the Commonwealth Information Security Center (JMU) collaborate to design and promote the adoption of such program which will include training needs and other parameters.

6. Health and Medical Improvements

BACKGROUND:

The Health and Medical Sub panel held its first meeting on April 25, 2002. That meeting included presentations concerning the response to the attack on the Pentagon and to the anthrax outbreak. The Sub panel was also briefed on terrorism preparedness and response planning that is ongoing in different regions of the State. In addition, the Sub panel presented a proposed work plan.

A second meeting was held on May 30. At that meeting, the sub panel received five presentations concerning 1) the findings, recommendations and outstanding issues from Governor Gilmore's Virginia Preparedness and Security Panel; 2) terrorism consequence management planning in Virginia; 3) legal issues related to terrorism preparedness; 4) terrorism-related issues currently facing the state laboratory; and 5) the status of the Department of Health's application for bioterrorism grant funding from the Centers for Disease Control and the Health Resources and Services Administration. The Sub panel's next meeting is scheduled for June 19.

One topic that the sub panel has identified involves the state's capacity to provide critical incident stress debriefing and crisis counseling services in the aftermath of a terrorist attack. At the request of the sub panel, the Secretary of Health and Human Resources has directed the Department of Mental Health, Mental Retardation, and Substance Abuse Services, and the Department of Health, to analyze the state's capacity to provide these services, and report to the sub panel on any gaps or shortfalls in this capacity. This report is expected in the near future.

The sub-Panel developed the following recommendations, which are being acted on:

ACTION:

I. The Governor is asking the Attorney General to provide an opinion concerning whether the State has sufficient legal authority to respond to a public health emergency in the following ways:

- Suspension of health professional licensure requirements (including those for out-of-State and retired health care professionals),
- Enforcement of quarantines, and
- Public taking of private resources, including medical personnel and supplies, for emergency response.

II. As a result of legislation (SB59) enacted during the 2002 Session, the Virginia Board of Medicine is required to collect and maintain, for the sole purpose of expedited dissemination of information about a public health emergency, telephone numbers, and e-mail addresses or facsimile numbers for all of its licensees. The collected information is not to be made available for any purpose other than the public health emergency. The Code of Virginia should be amended to require all of the State's other health regulatory boards (e.g., nursing, pharmacy and psychology) to

collect and maintain this same type of information for the sole purpose of expedited dissemination of information about a public health emergency. The collected information would not be made available for any other purpose. This requires amended legislation, which will be pursued.

III. The Governor has advised Secretary of Health and Human Resources to establish a task force to study certain issues concerning medical malpractice, as it relates to bioterrorism response preparedness. The following issues should be studied:

- How will medical malpractice insurance coverage be provided, and by whom, to physicians who close their offices in order to respond to an emergency at another location, and are thereby unavailable to treat their regular patients?
- How will medical malpractice insurance coverage be provided, and by whom, to physicians who are unable to provide the usual and customary standard of care during an emergency response due to the lack of proper space, supplies and equipment?
- To what extent does Virginia's "Good Samaritan" statute (§8.01-225 of the Code of Virginia) provide liability protection to health care practitioners who provide services in response to a public health emergency?